Following Data Through Layers 2, 3, and 4

Cybersecurity

Networking 101, Day 3

Class Objectives

By the end of today's class, you will be able to:

- Define enumeration as a set of methods used by security professionals and hackers to determine network vulnerabilities.
- Use Wireshark to visualize and analyze ARP activity, including ARP spoofing.
- Use `ping` and `fping` to determine if hosts are operating and accepting connections.
- Use `traceroute` to troubleshoot networking communication issues between two devices.
- Define and distinguish between TCP and UDP.
- Analyze TCP traffic in Wireshark.
- Analyze SYN Scans to determine the availability of ports on a network.

Hackers will often try to gain unauthorized access into a network. It's the job of security professionals to secure networks by identifying vulnerabilities.

Real World Hacking Example

- A hacker may discover that a server with payroll data accidentally has open port 22, for SSH.
- This lets the hacker gain unauthorized access to the network, allowing them to steal or alter important data, e.g., social security numbers or salary information.
- It is the security professional's job to determine which unauthorized ports are open, and then close them, thus protecting the integrity of the company.

Enumeration

Both hackers and security pros will use the method of enumeration to gather data from a specific network in order to gain access to that network.

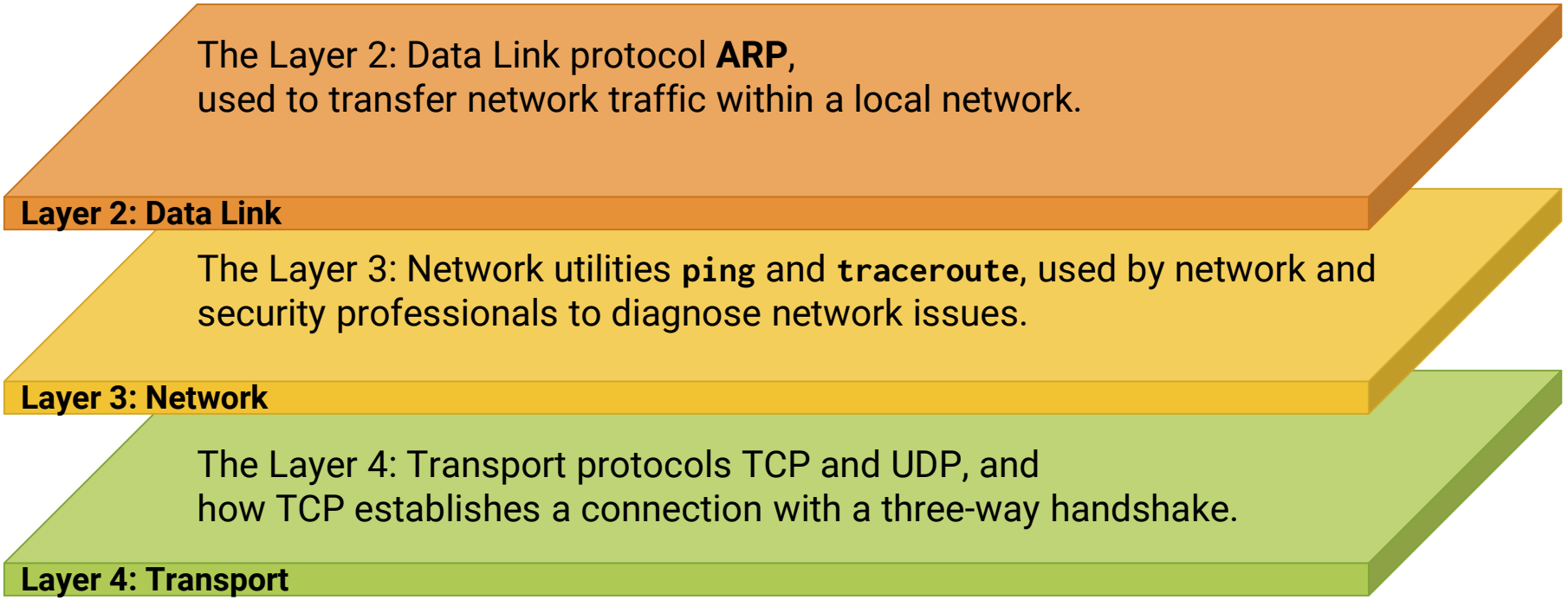
Enumeration

Enumeration can yield the following information:

- Physical addresses of devices within a network.
- The IPs and ports that are being used or are accessible.
- Network and network security devices being used.

Moving Through the Layers

Today, we'll move through three important OSI layers and their corresponding tools and protocols:



Media Access Control (MAC)

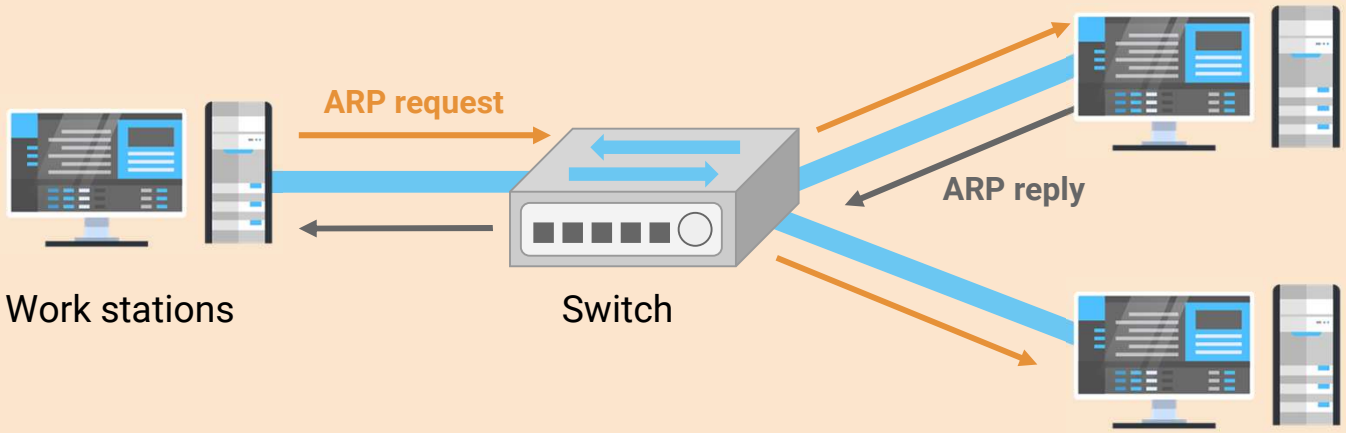
When data travels from a WAN to a LAN, it still needs to find its final destination *within* the LAN.

Data is routed via switches to a physical machine address, known as a **Media Access Control (MAC)** address:

A sequence of numbers such as `00:0c:29:0f:71:a3` that identifies the destination computer's unique hardware number.

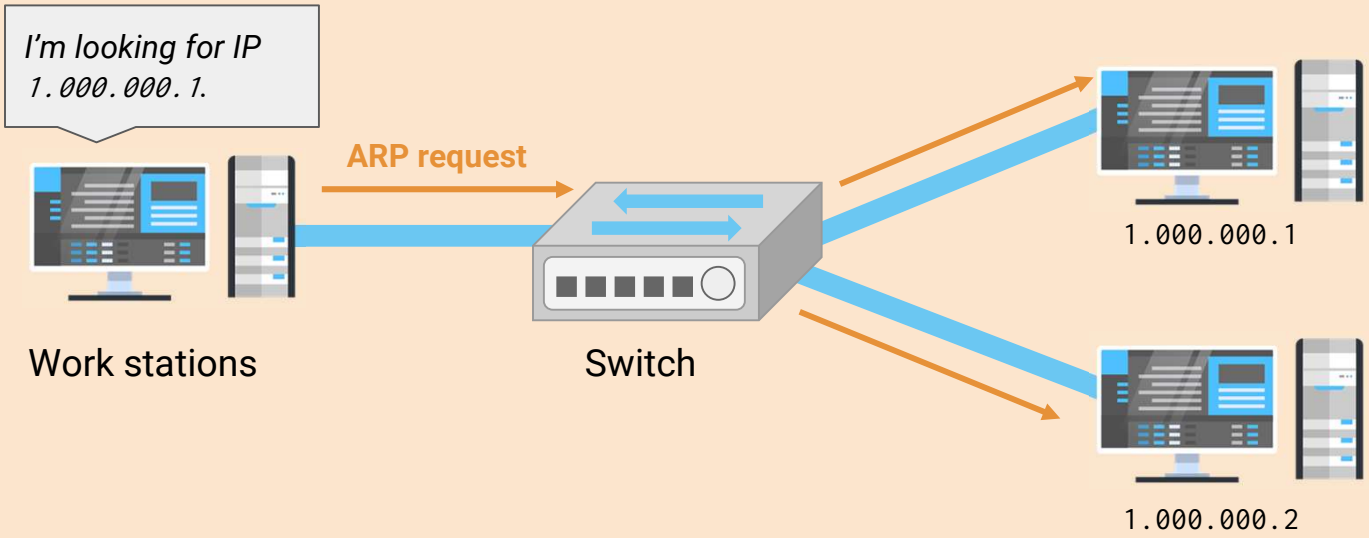
Now Entering Layer 2: Data Link

To ensure data gets from LAN to machine, the Address Resolution Protocol (ARP) maps the MAC address to an IP address within the LAN.
This mapping is known as **ARP request and reply**.



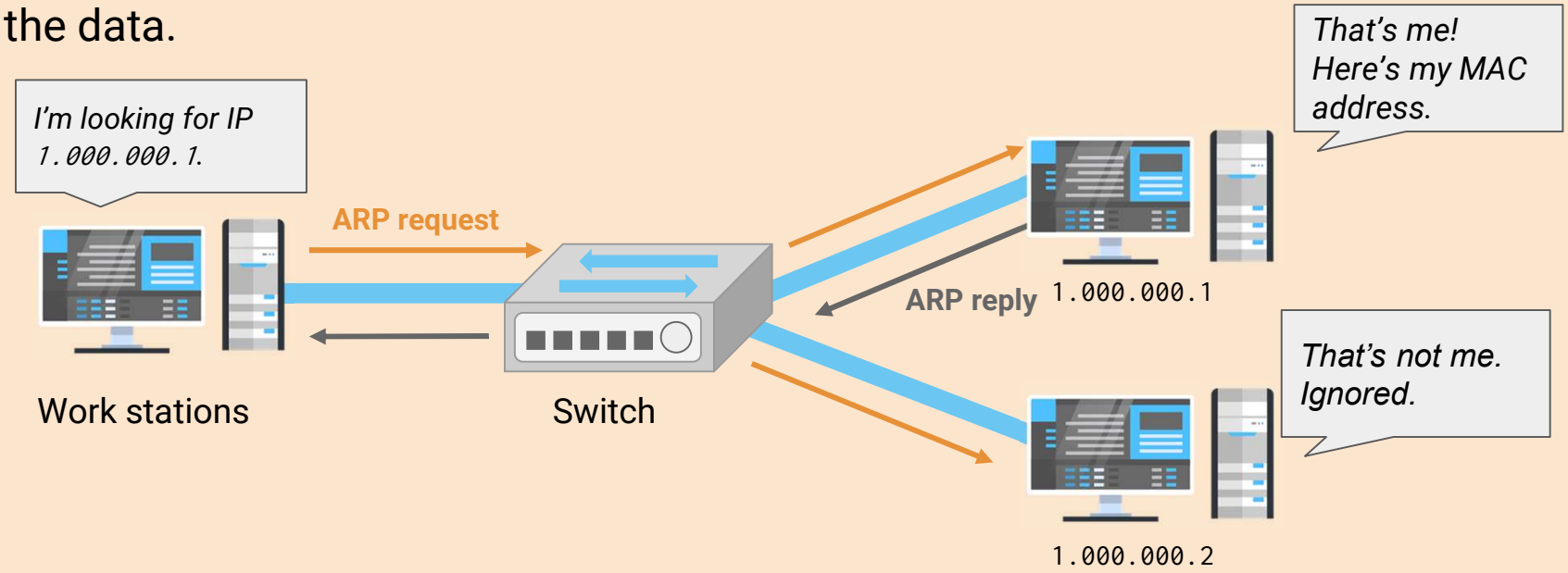
Now Entering Layer 2: Data Link

Request: The network device transmitting the data broadcasts an ARP request to all devices in its network to find the physical address matching the IP address.



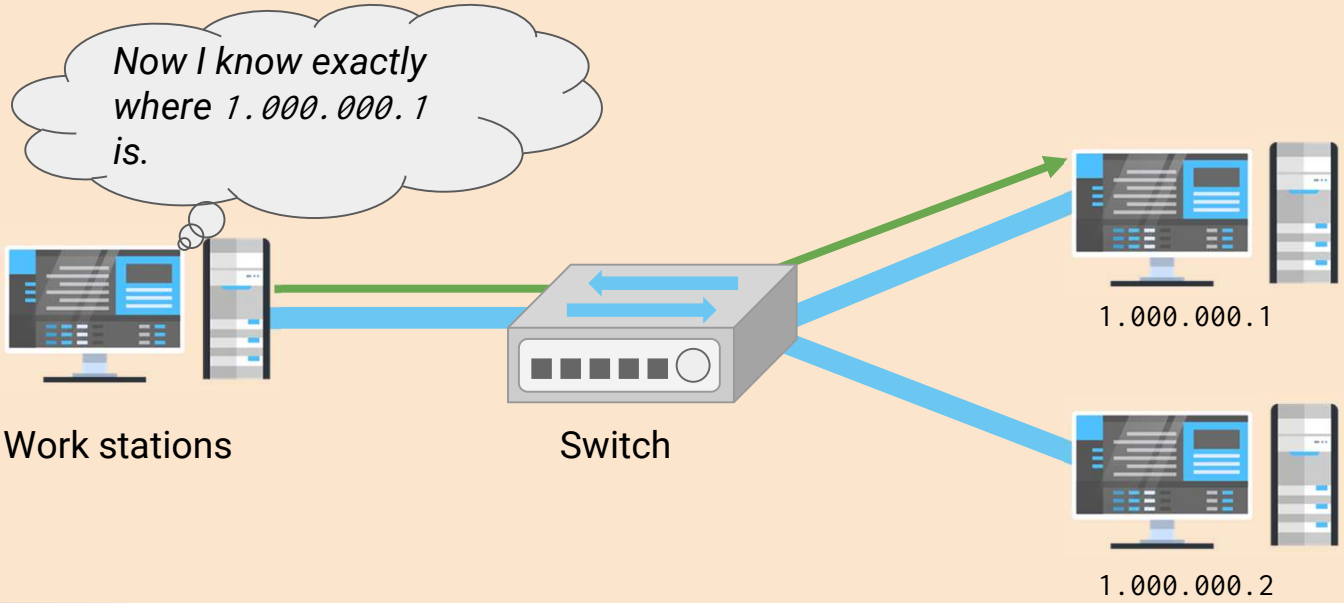
Now Entering Layer 2: Data Link

Reply: The device owning that IP address recognizes their IP in the ARP request and sends an ARP reply with their MAC address so the network knows where to route the data.



Now Entering Layer 2: Data Link

The mapping of the MAC address to the IP address is added into the ARP cache. The next time data comes in for this specific destination, it won't need to broadcast an ARP request. The network has the record in its cache, and can automatically route the data.



ARP Cache Timeout

Entries added to the ARP cache are called **dynamic** ARP entries, meaning they can be changed with future ARP replies.

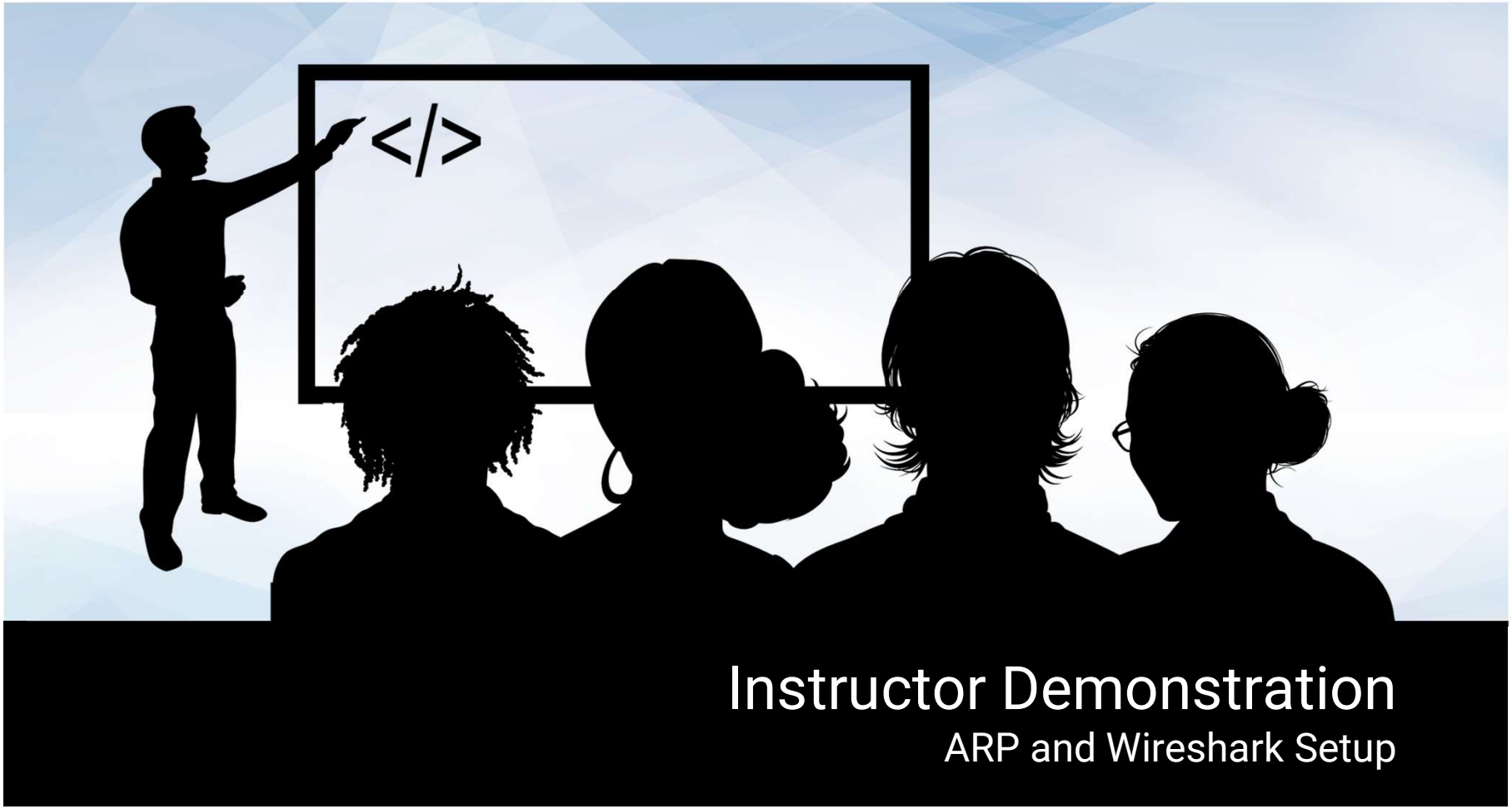
Dynamic ARP entries will only stay in the ARP cache for a limited period of time known as the **ARP cache timeout**.

When the ARP cache timeout expires, the record is removed from the ARP cache and any future requests for the host require a new ARP request.

ARP and Wireshark Setup

Wireshark lets us visualize ARP requests and responses. In the next demo, we will:

- Filter for all ARP packets in a .pcap file.
- This filter will show us the request from the source host, which will include a MAC address, associated with a specific IP address, that the data needs to be transmitted to.
- If the request can be successfully answered, we'll see a response from the owner of the IP address, containing the device's MAC address.



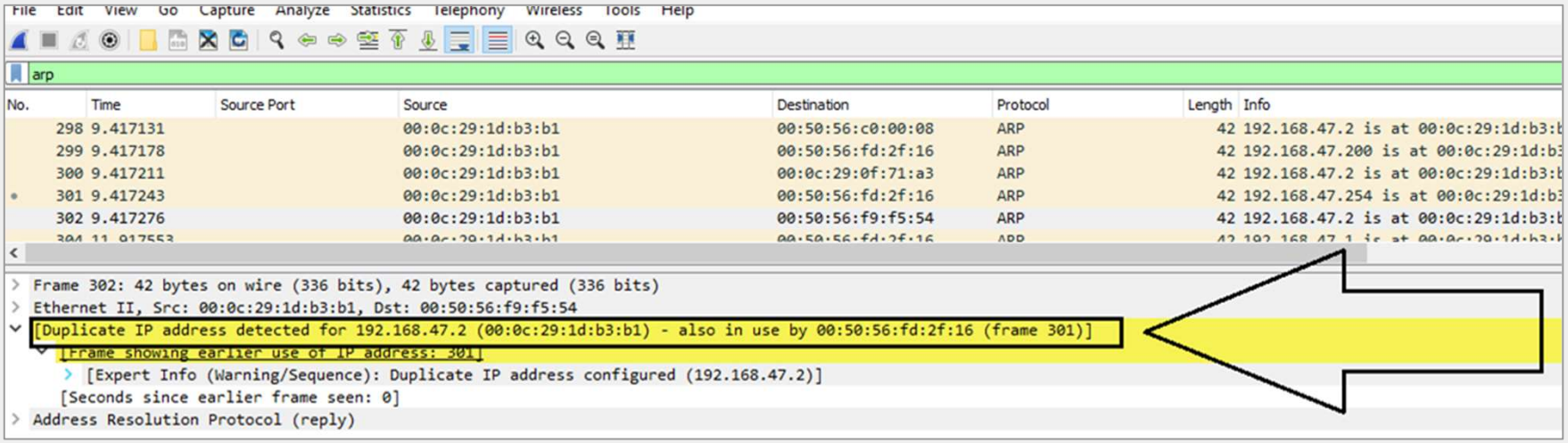
Instructor Demonstration

ARP and Wireshark Setup


ARP and Security
If a hacker has access to a LAN, they can intercept traffic on its way to the correct destination (“the good host”).

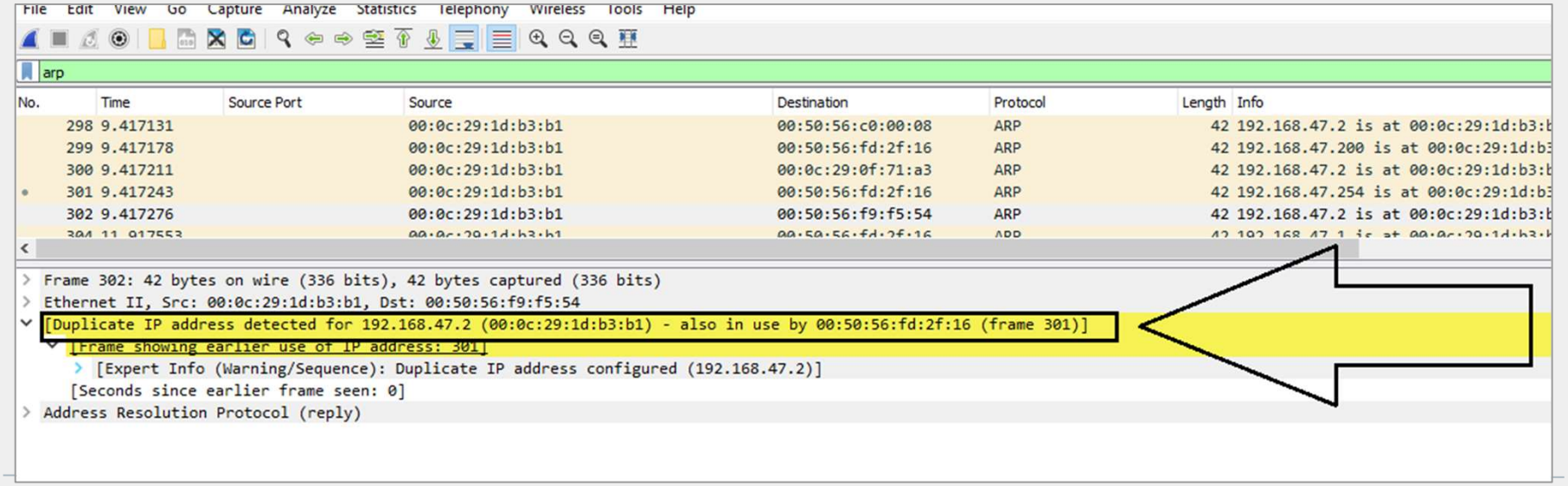
ARP Spoofing

- The hacker can send a spoof ARP message to the LAN, directing all traffic intended for the good host to the hacker's MAC address.
- After the attacker sends the spoof ARP message, all traffic originally destined for the good host is intercepted by the hacker’s device with the malicious MAC address.



ARP Spoofing

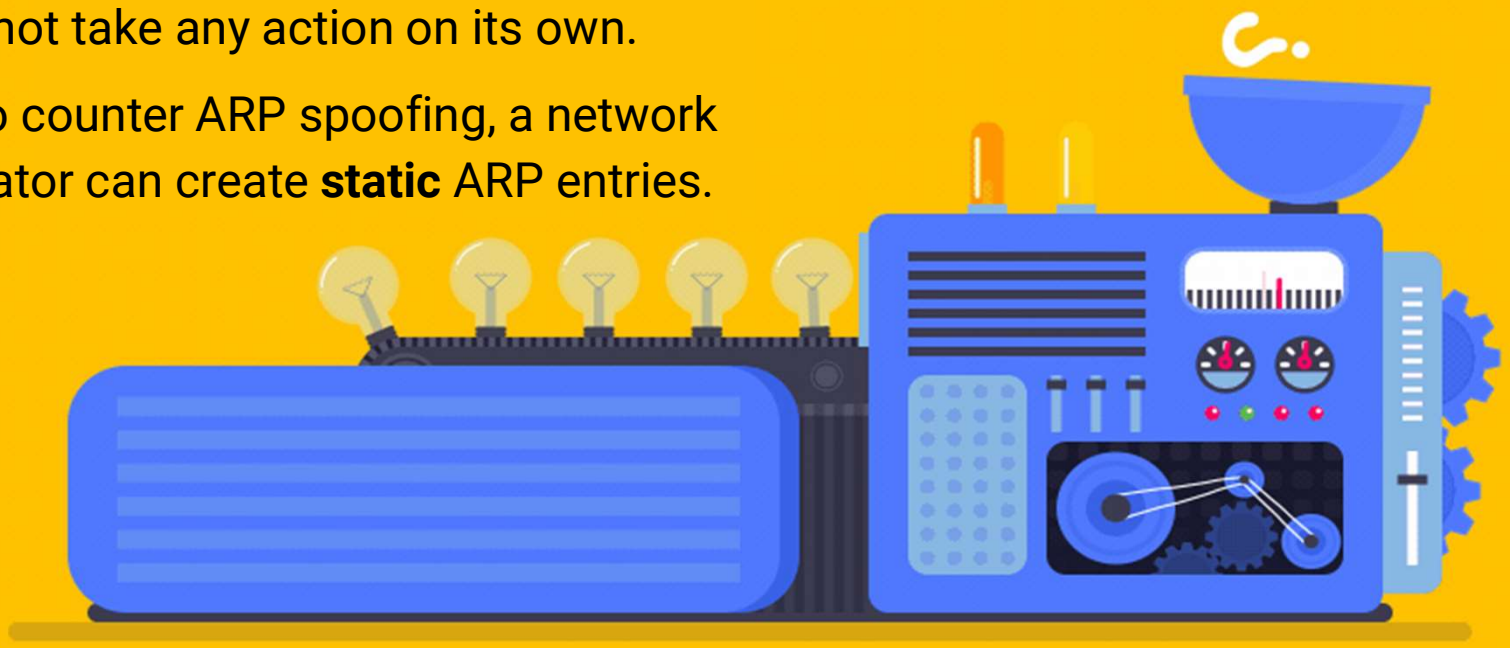
- The good host is **`192.168.47.20`**; the correct MAC address is **`00:50:56:fd:2f:16`**.
- The hacker's MAC address is **`00:0c:29:1d:b3:b1.`** A spoof ARP message directs traffic intended for the good MAC address to the hacker's MAC address.
- The spoof ARP message can be understood as: **`192.168.47.2 is at 00:0c:29:1d:b3:b1.`**



But There's a Solution!

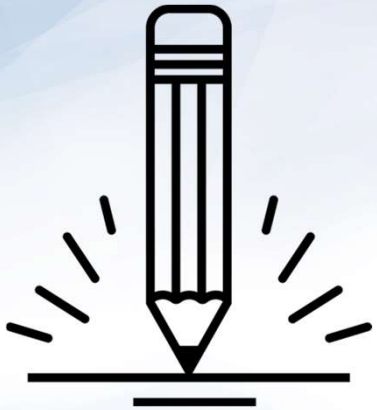
Wireshark can detect and alert multiple MAC addresses associated with a single IP address, but it will not take any action on its own.

Instead, to counter ARP spoofing, a network administrator can create **static** ARP entries.



Static ARP Entries

- Static ARP entries create permanent IP-to-MAC-address mappings in the ARP cache.
- Unlike the dynamic ARP entries, these cannot be changed.
- All IP-to-MAC address mappings of all hosts on a network must be known ahead of time.
- It’s time-consuming to enter each IP-to-MAC mapping in the ARP cache, and these need to be continuously maintained as hosts get added or changed.



Activity: Analyzing ARP Activity

In this activity, you will play the role of a security analyst at Acme Corp.

Your task is to analyze ARP activity from a CompuCom packet capture to determine if any vulnerabilities exist.

Suggested Time:
15 minutes

Time’s Up! Let’s Review.

`ping`

(Packet Inter-Network Groper)

When enumerating, it’s important to check if an external host is operating and accepting connections.

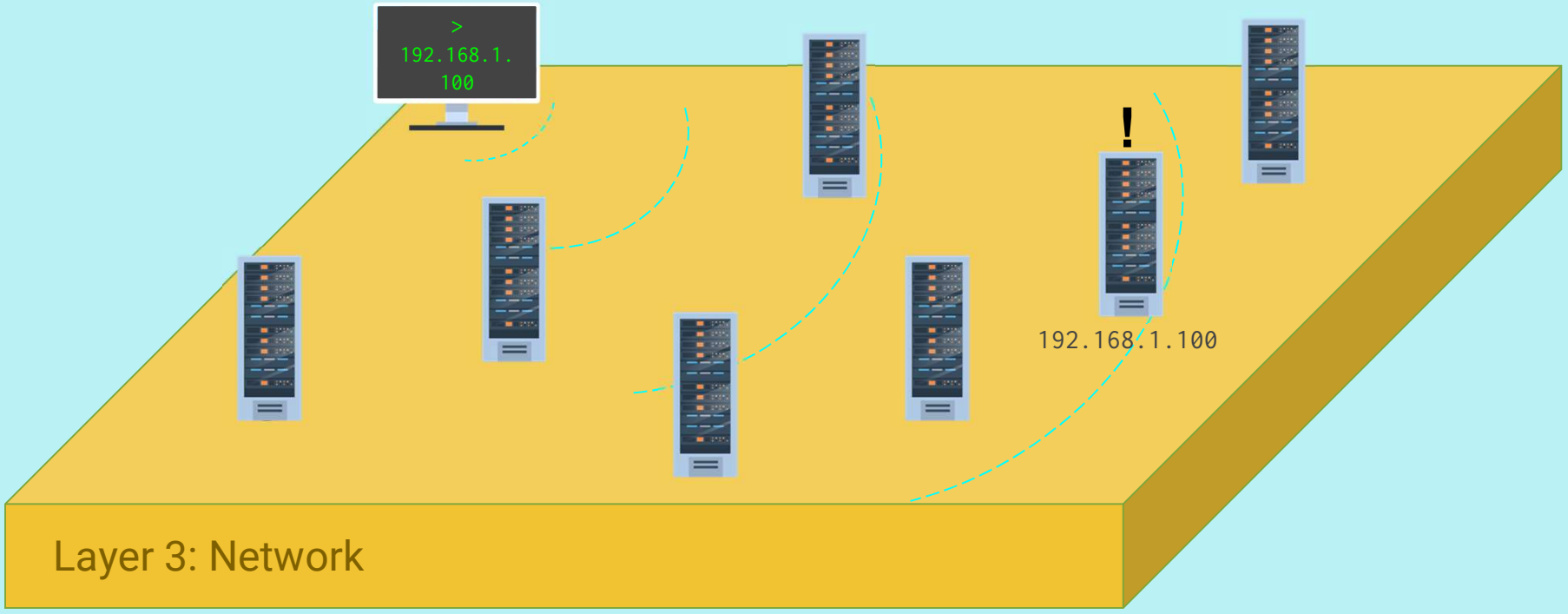
`ping` Example

Company X wants to make sure their new intranet is accessible from their offices in the United States and Japan. The intranet is used for daily employee tasks and to access employee contact information. So availability of the intranet is critical for all employees.

- To test the accessibility to the intranet, Company X might have employees from the United States and Japan each send a `ping` request from their location to validate the intranet is available and accessible from each location.

Now Entering Layer 3: Network Layer

`ping` (Packet Inter-Network Groper) is a utility used to determine if a host is operating and accepting requests.



Internet Control Message Protocol

When we ping a host, it sends an **Internet Control Message Protocol (ICMP)** echo request to a specific IP address and waits on a reply.

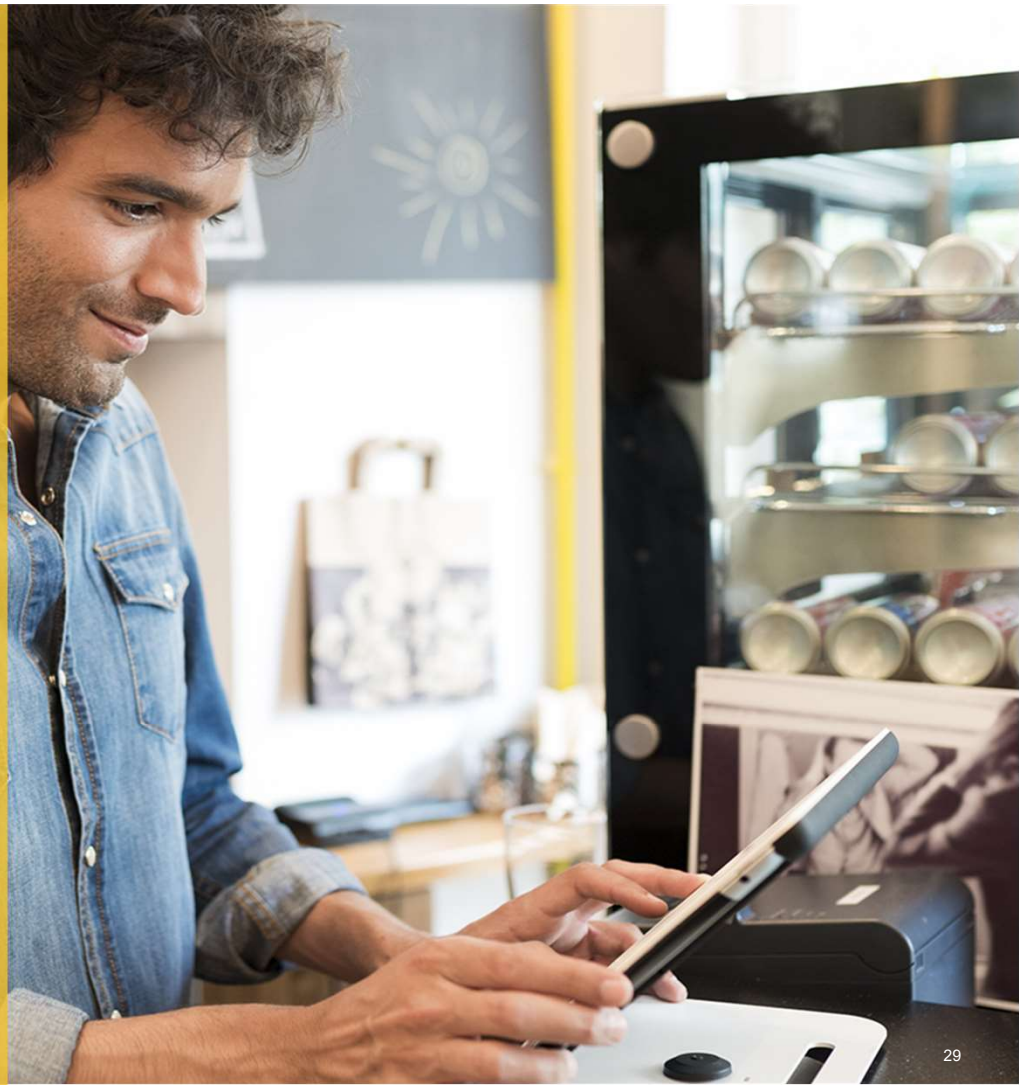
- ICMP is a protocol that network devices use to send error messages and operational information about whether a requested service or host can be reached.

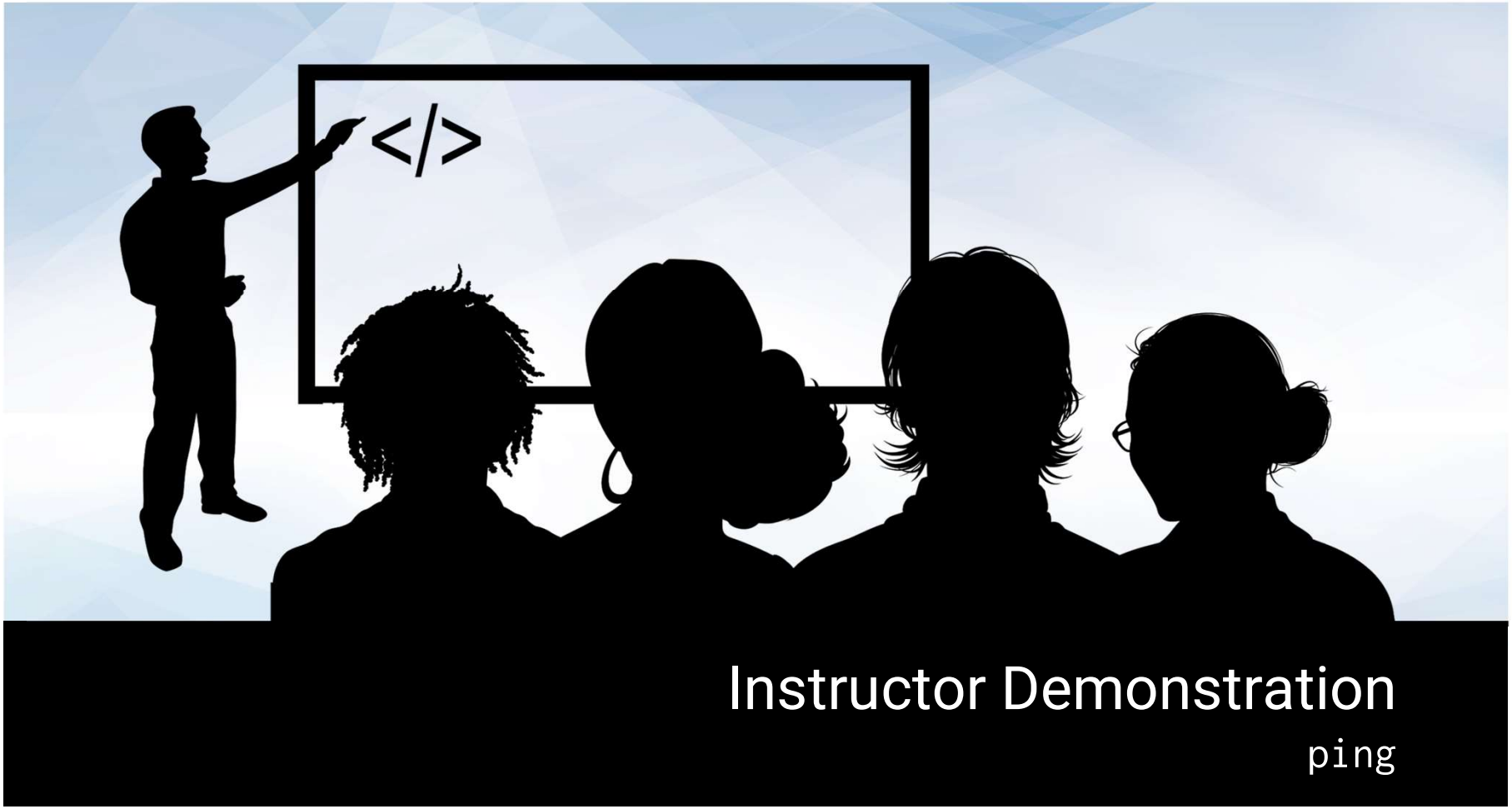
`ping` Demo Scenario

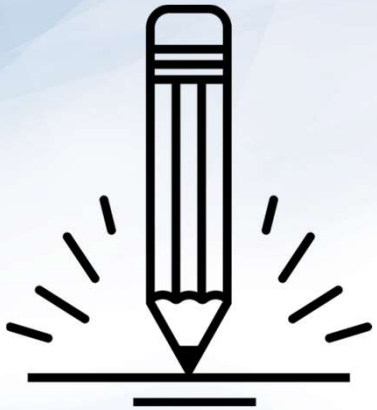
In the following demonstration, we'll use `ping` on the command line with the following scenario:

- We are a restaurant looking to purchase commercial beverages online.

  We need to check if Pepsi.com is working and accepting requests.




Instructor Demonstration
ping



Activity: Enumerating with `ping`

In this activity, you will continue to play the role of a security analyst at Acme Corp.

You must use `ping` to determine which of CompuCom's host IP addresses are accepting connections.

Suggested Time:
15 minutes

Time’s Up! Let’s Review.

Countdown timer

15:00

(with alarm)

Introduction to traceroute

`traceroute` Demo

In the previous demonstration, we discovered that redbull.com was not accepting requests.

Now we'll find out why.

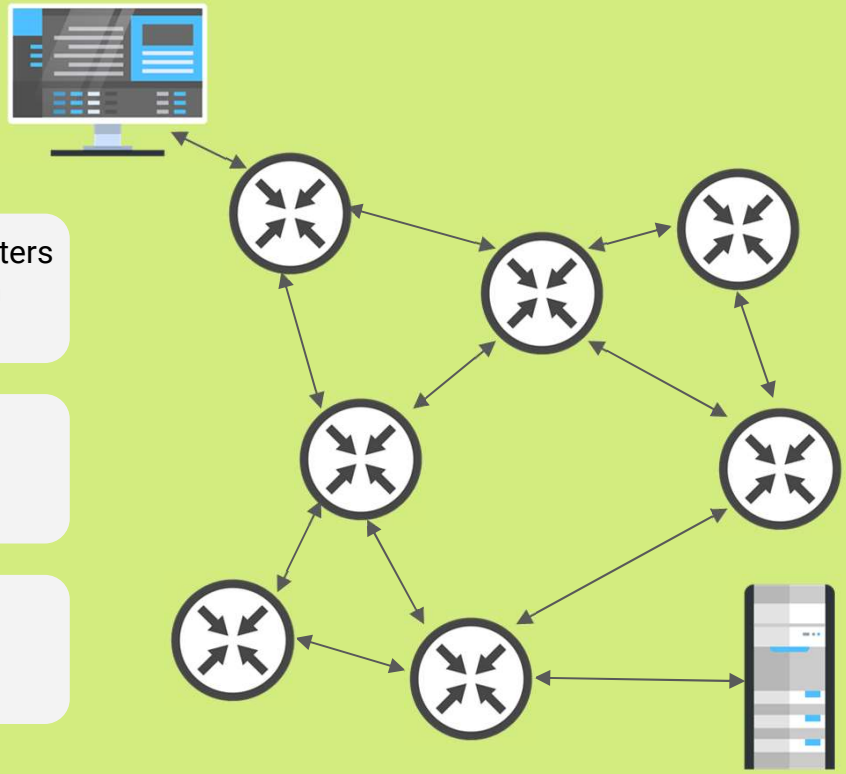
While `ping` indicates if a host is up or down, security professionals will often need more info to determine *why*.

Company X's employees were able to successfully ping their intranet from the United States office, but unable to ping the exact same address from the Japan office.

- More information is needed to understand why the intranet is not accessible from Japan.
- Company X can better understand the issue by finding out where in the request the failure occurred.

Routing and Redirections

When data travels from a source to a destination, it typically doesn't follow a straight path.



Data is often redirected by many routers. Routers connect different networks so their hosts can communicate.

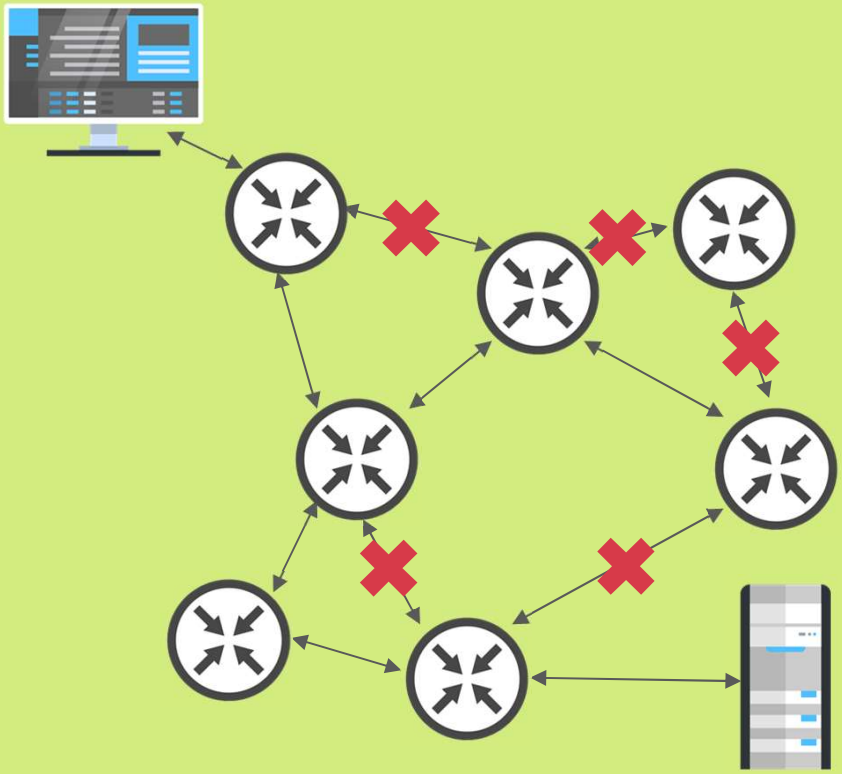
Redirection of data transmissions are called **hops**.

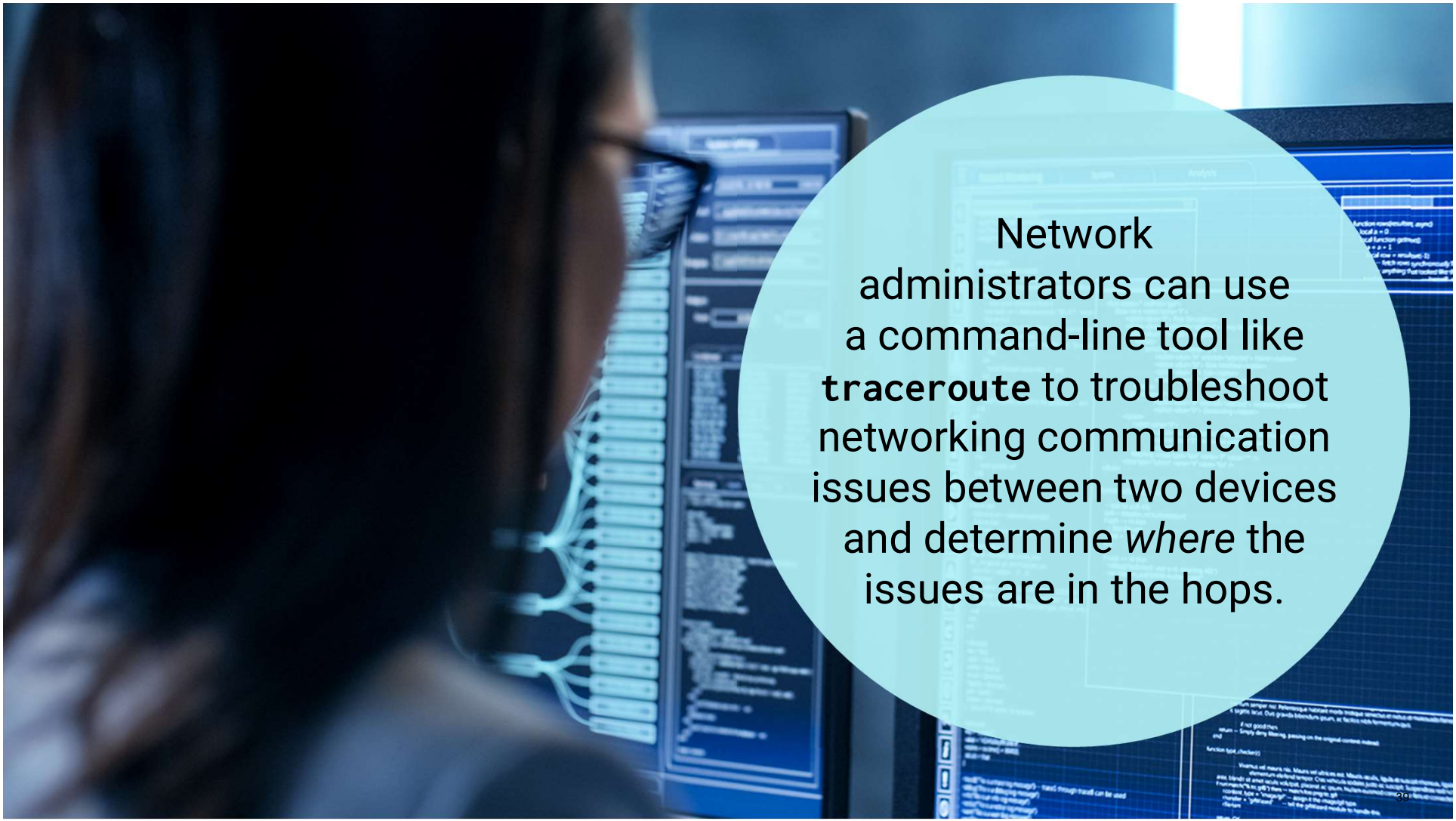
Optimal routing paths are determined based on the "shortest path," which is influenced by network topology.

Routing and Redirections

Despite using the “shortest path,” communication between two devices can sometimes fail, leaving network administrators unsure where a communication problem is located.

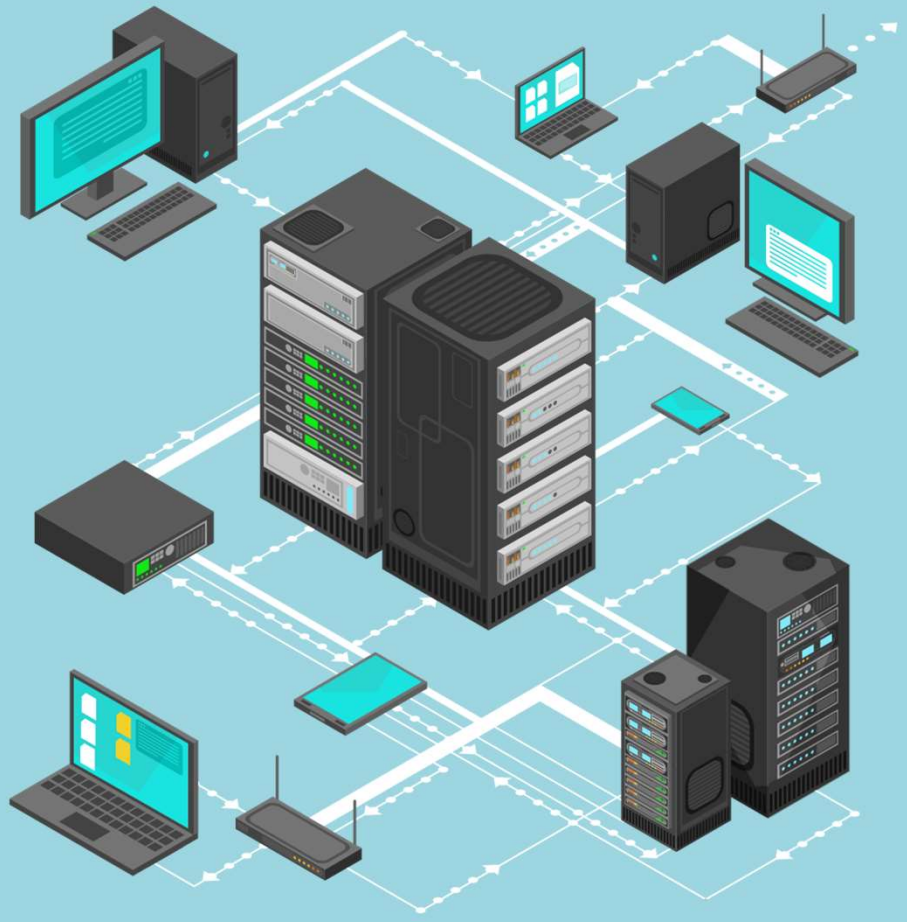
Poor connectivity and latency problems are often due to packets being dropped along their routing paths.




Network administrators can use a command-line tool like **traceroute** to troubleshoot networking communication issues between two devices and determine *where* the issues are in the hops.

Introduction to `traceroute`

- `traceroute` shows the route taken between two systems across a network.
- It lists all routers (hops) the connection must pass through to get to the destination.
- Network administrators can use `traceroute` to identify precisely where connectivity problems occur.



`traceroute` Uses

In addition to troubleshooting connectivity issues, `traceroute` can be used to:

Display how systems are connected, or map the network.

Generate baseline profiles of the network.

Diagnose poor network performance issues.

ICMP and Time to Live (TTL)

Like `ping`, `traceroute` also utilizes the ICMP protocol. It also shows the time taken to travel across each of these hops, from source to destination.

The ICMP header contains a field called **Time to Live** (**TTL)**:

01

TTL is an indicator of how long a data packet can exist in a network.

02

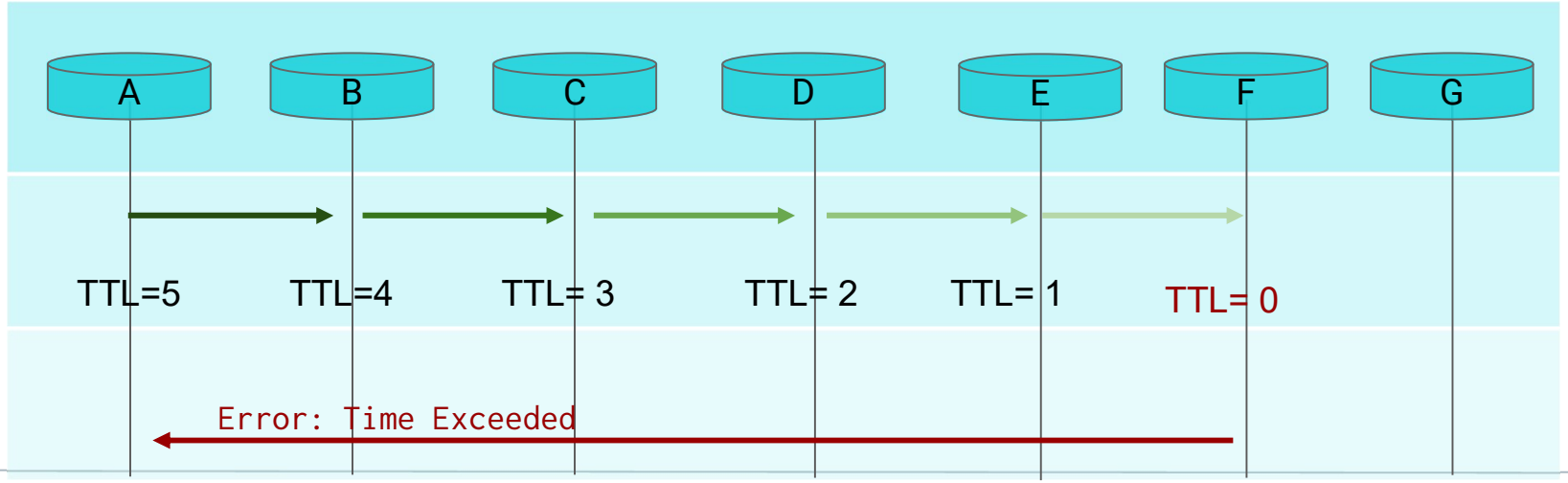
TTL is utilized as a decrementing hop counter.

Every router that forwards the packet decrements (reduces) the TTL value by one.

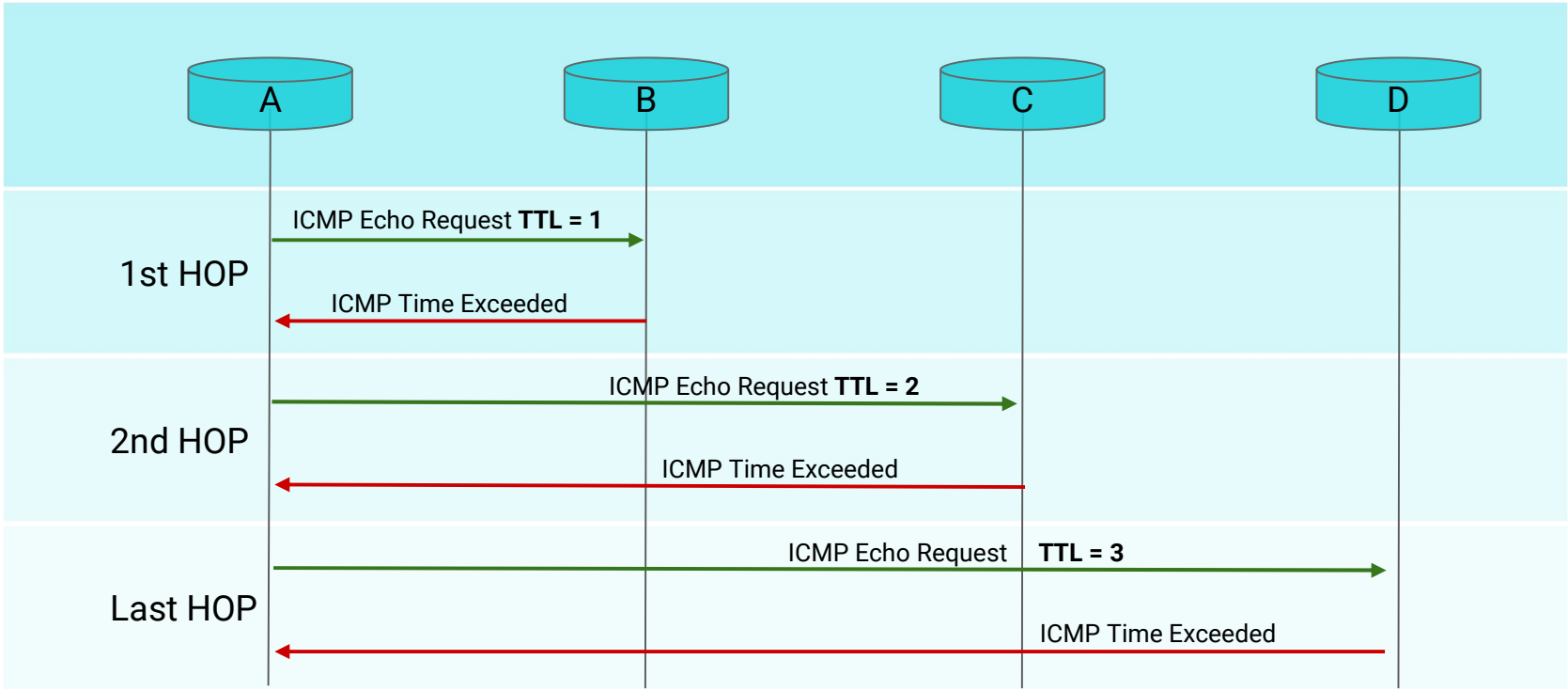
Time to Live (TTL)

If the starting TTL value of a data packet is **five**, and the data travels across **two** routers, the TTL will drop to **three**.

- When the TTL count reaches zero, it sends a "time exceeded" error message back to the source address.
- This prevents data from being stuck in an infinite loop if it's unable to be delivered to the destination.

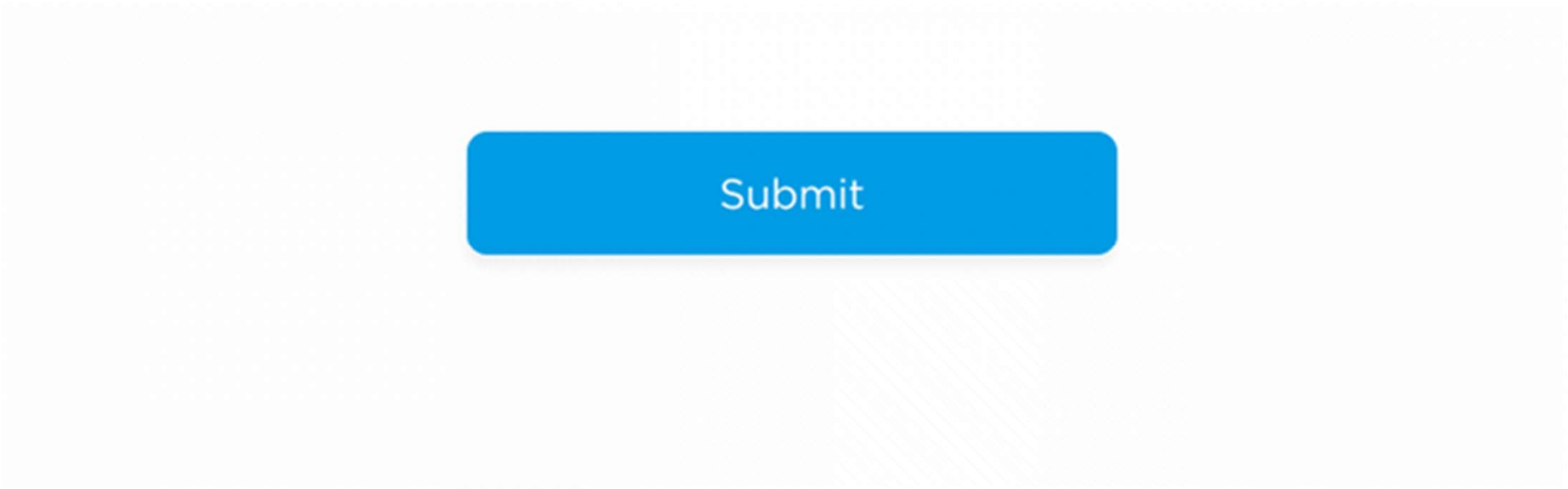


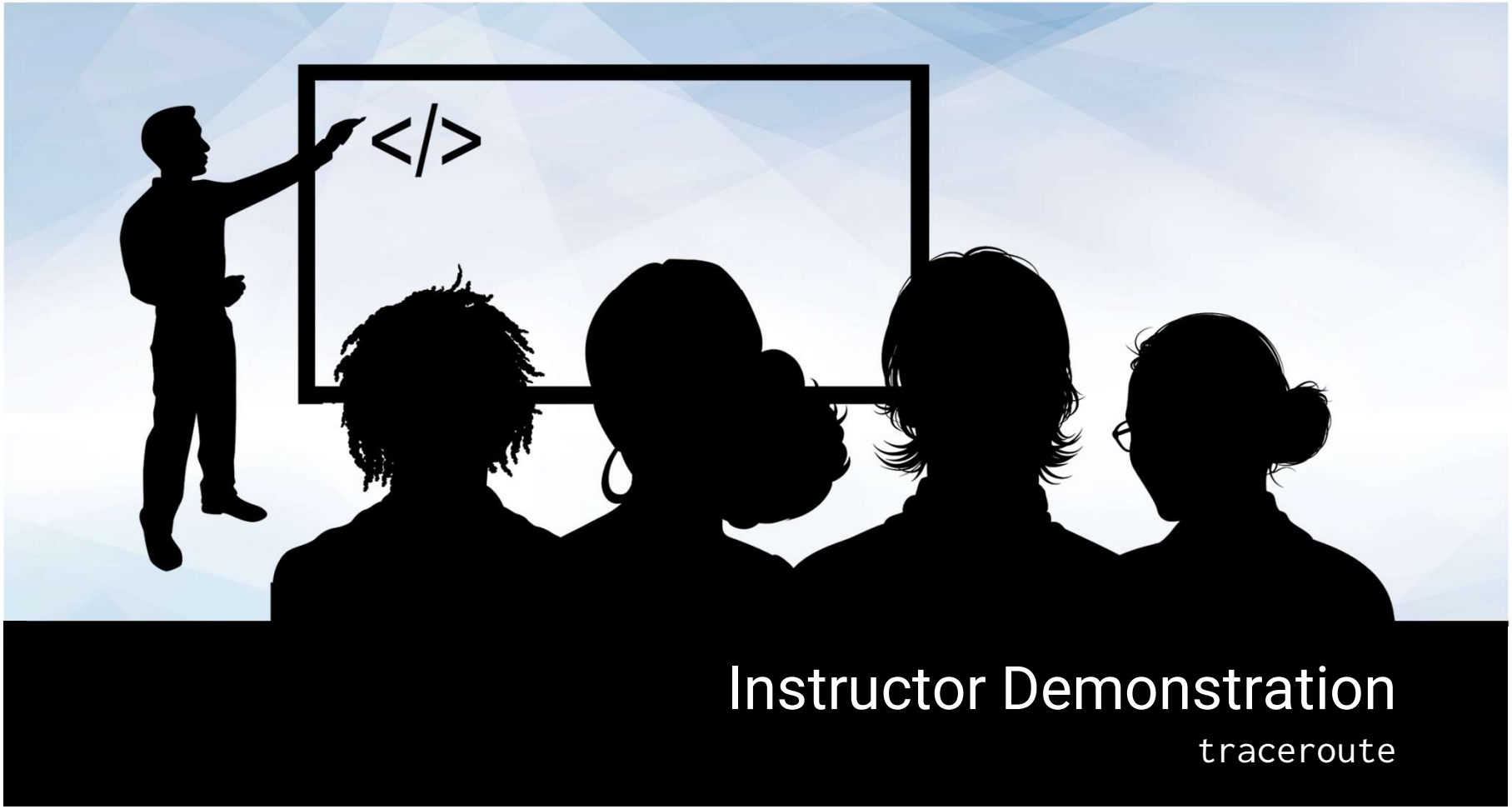
User Datagram Protocol (UDP)

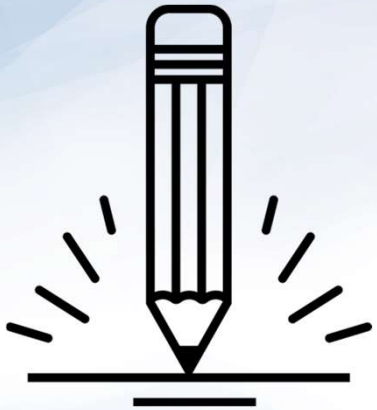


Traceroute Demo

Now we'll use traceroute on the command line to further investigate why **redbull.com** isn't responding.




Instructor Demonstration
traceroute



[Optional] Activity: Enumerating with `traceroute`

In this activity, you will continue to play the role of a security analyst at Acme Corp.

You've been tasked with further analyzing the IPs rejected in the last activity to determine where in their path the connection is being dropped.

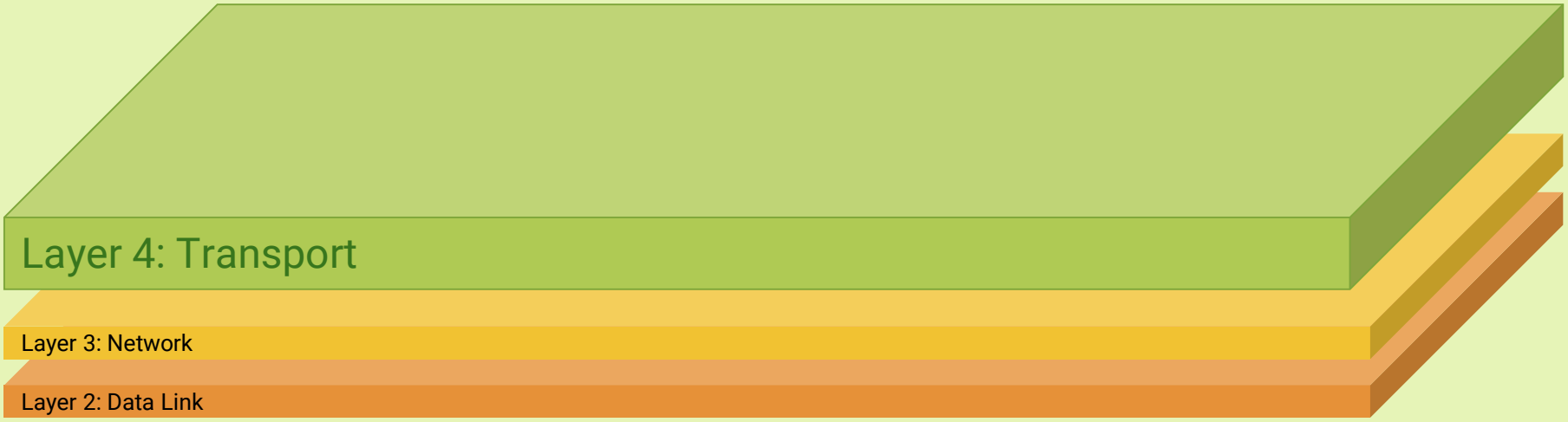
Suggested Time:
Complete if class falls on a Saturday

Time’s Up! Let’s Review.

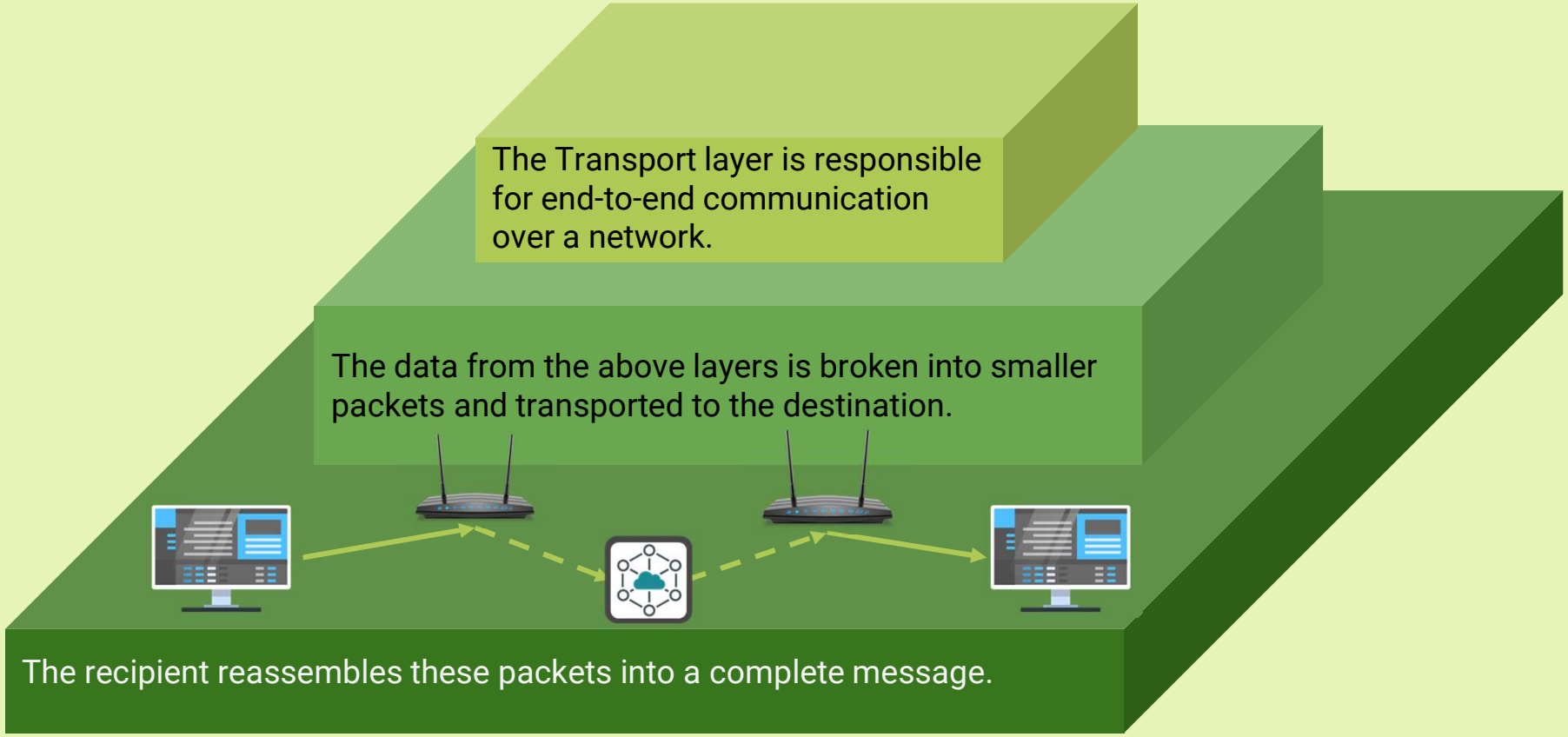
Checkpoint

So far, we've studied the ARP protocol on Layer 2 and the `ping` and `traceroute` utilities from Layer 3.

Now, we'll move onto Layer 4 protocols **TCP** and **UDP**.



Layer 4: Transport Refresher



TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) is one of the most widely used protocols for data transmission.

It is a “connection-oriented” protocol, meaning the server must acknowledge it has received the request from the client.

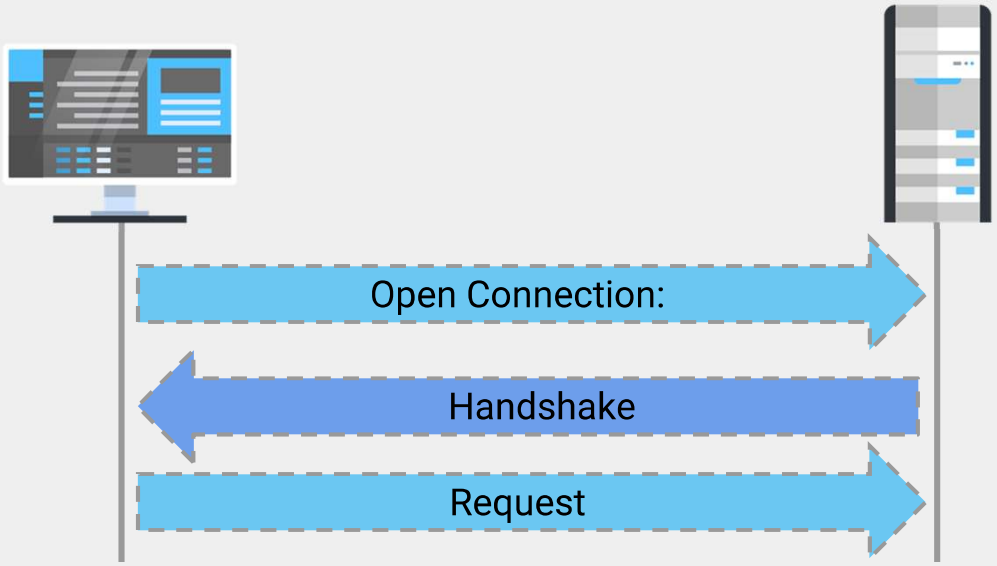
If the recipient doesn’t acknowledge the request, the sender assumes the request has not been received and will attempt to resend.

This connection-oriented acknowledgment is known as the **TCP Handshake.**

TCP in the Real World

TCP also ensures that all data is transmitted without errors, in the correct order.

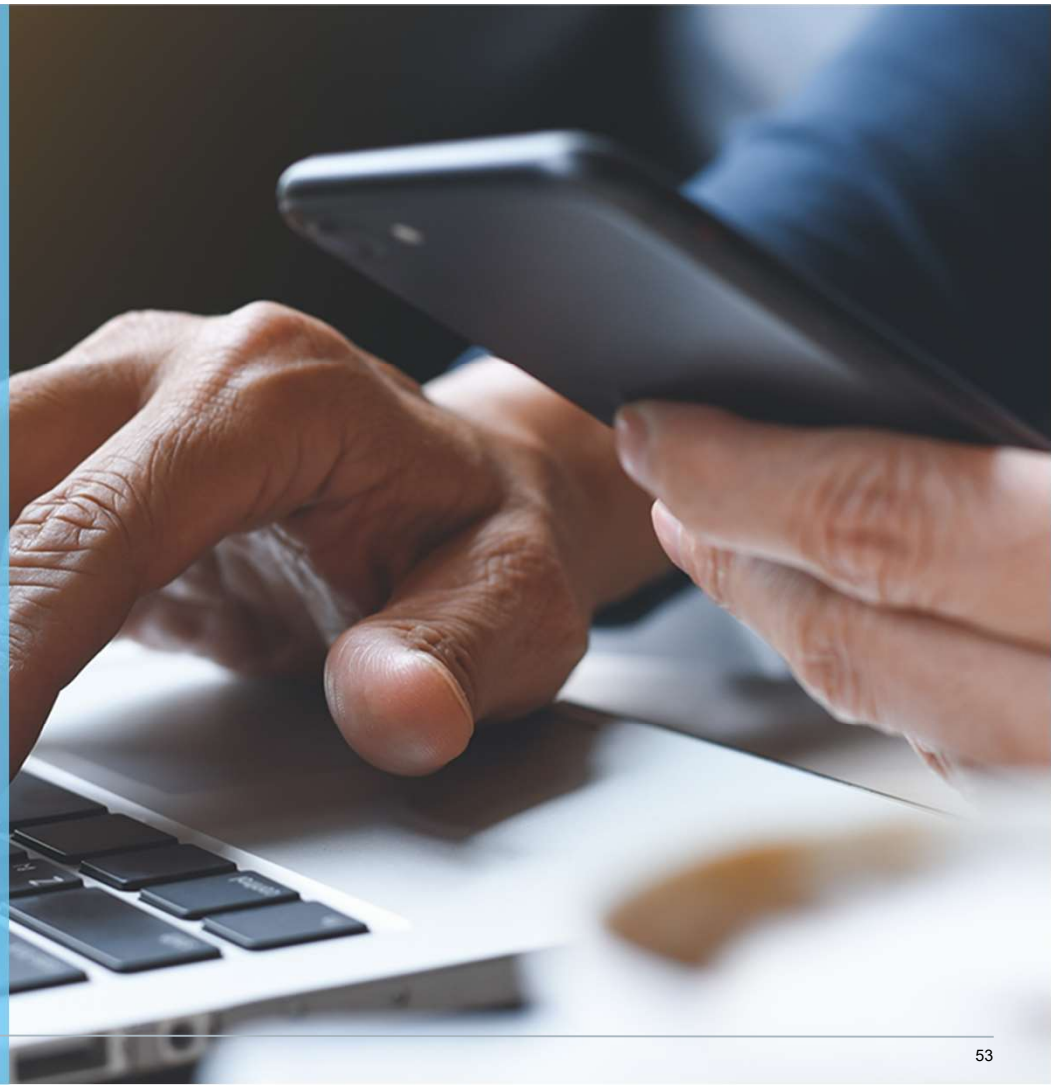
TCP is used with familiar protocols such as HTTP, HTTPS, FTP, SSH, and SMTP.



TCP in the Real World

For example: We want to check our transaction history on an online banking website.

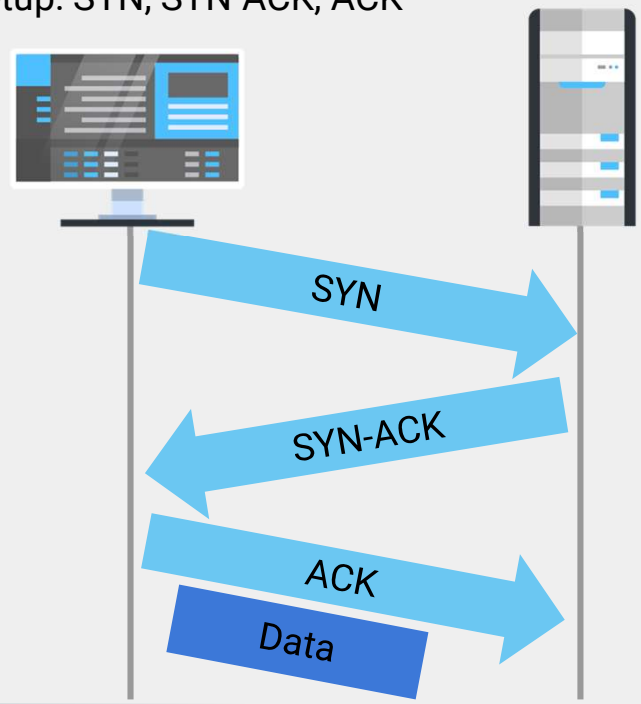
- We would use HTTPS, a protocol that runs over TCP. It ensures that all the requested data from our banking transaction history has been transmitted from the bank's web server.
- Banking customers need to trust the integrity of the data they are viewing. It’s critical that banking data is complete and error free.



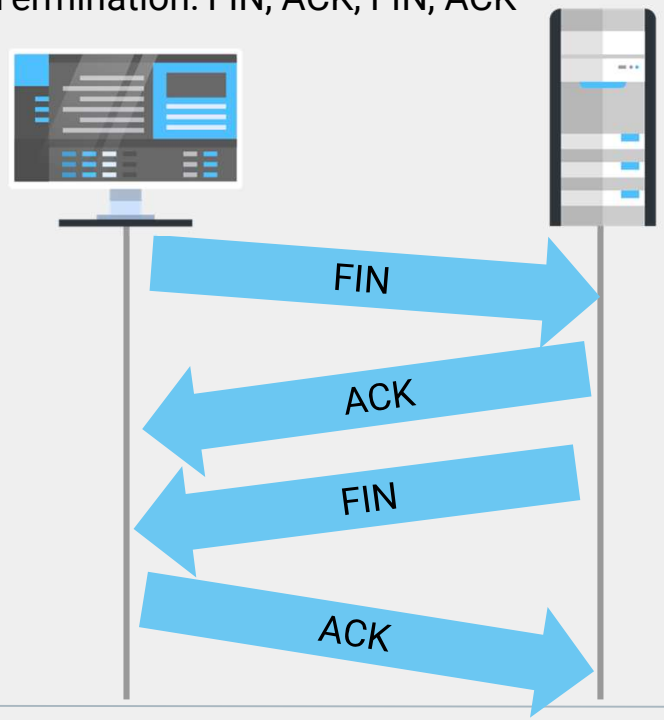
Three-Way Handshake

The TCP three-way handshake is the process that lets both sides know data has been transmitted completely.

Setup: SYN, SYN-ACK, ACK



Termination: FIN, ACK, FIN, ACK



Three-Way Handshake: Step by Step

01

SYN (*synchronize*): From client to server. Client sends a SYN data packet to the server to determine if it is ready to open a connection.

02

SYN/ACK (*synchronize/acknowledge*): From server to client. The server acknowledges or confirms receipt of the SYN packet.

03

ACK (*acknowledge*): From client to server. Client confirms receipt of the SYN/ACK packet.

04

Once the handshake is successfully completed, the data transmission can begin.

Four-Way-Termination: Step by Step

01 **FIN (*finish*): From client to server.** The client sends a FIN data packet to the server to close the connection.

02 **ACK: From server to client.** The server acknowledges receipt of the FIN packet.

03 **FIN: From server to client.** After the server terminates the connection, it sends a FIN packet.

04 **ACK: From client to server.** The client acknowledges it has received the server's FIN packet. The TCP termination process is complete.

TCP Downsides

TCP also has disadvantages.

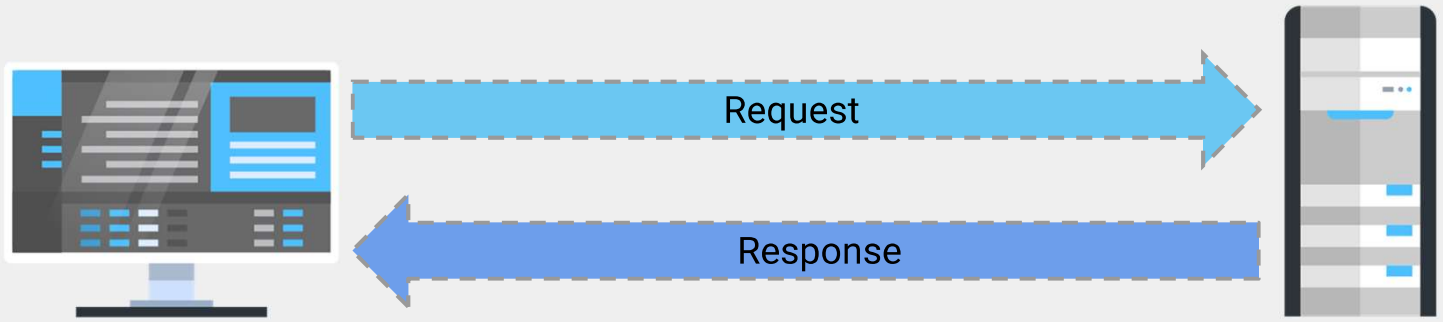
Retransmissions (when the server resends packets because the client does not acknowledge receipt) and the ordering of packets can cause delays during data transmissions.

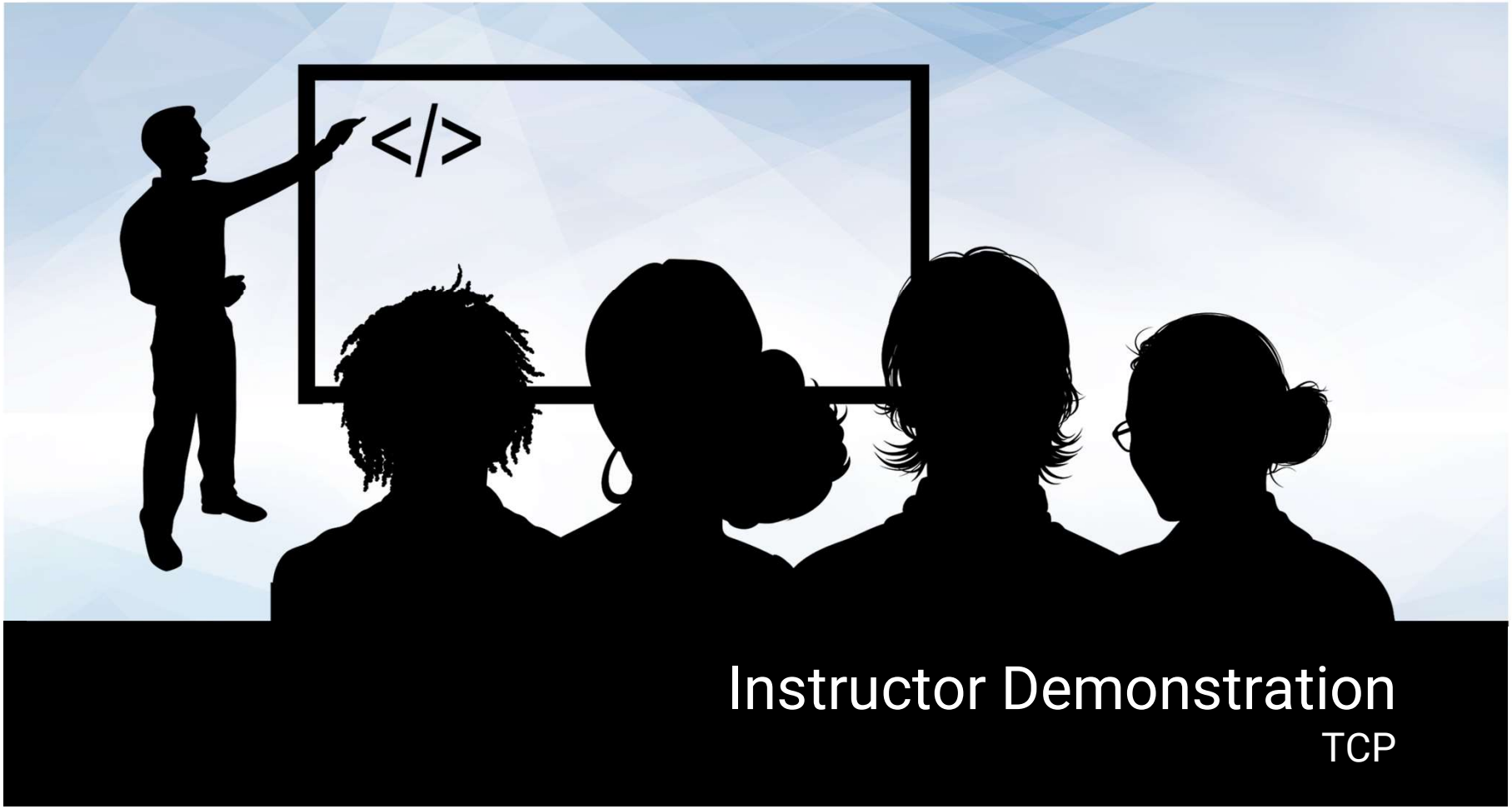
- In cases when every single packet of data does not need to be transmitted, TCP is not used. For example, streaming live video.

User Datagram Protocol (UDP)

For situations when it's not necessary for all data to reach the destination, there is the **User Datagram Protocol (UDP)**.

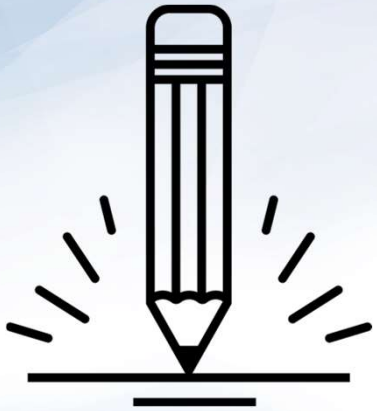
- UDP is better for reducing latency versus transmitting all data.
- UDP is a **connectionless** protocol—it doesn't require a handshake to transmit data.
- UDP simply sends off the packets. Its attitude is: *"If all the packets are received, great. If not, that's okay too."*





Instructor Demonstration

TCP



Activity: Analyzing TCP Traffic

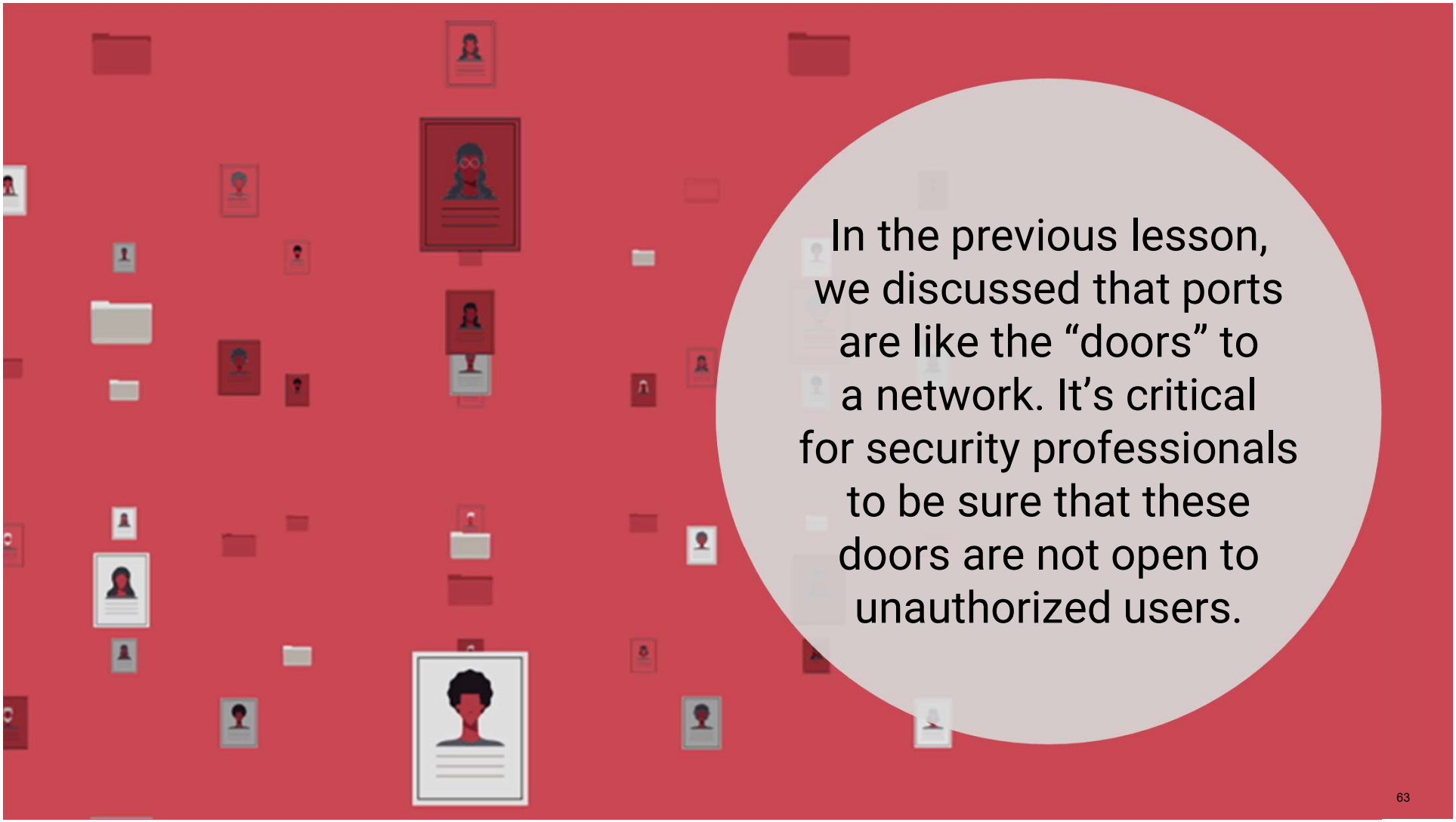
In this activity, you will continue to play the role of a security analyst at Acme Corp.

Your task is to analyze a new employee's TCP traffic to determine what they're working on during their first week.

Suggested Time:
15 Minutes

Time’s Up! Let’s Review.

Introduction to SYN Scan


In the previous lesson, we discussed that ports are like the “doors” to a network. It’s critical for security professionals to be sure that these doors are not open to unauthorized users.

Ports

Consider the following scenario:

- Company X recently set up a new network in its London office. A security administrator needs to ensure the only ports open on the machines are `80` (HTTP) and `443` HTTPS), since incoming and outgoing web traffic is allowed for their employees.
- If ports other than HTTP and HTTPS are open, there's a risk a hacker could access the network and view confidential info, or impact the availability of the network.

We can check for open ports on a network by sending a SYN request to every port on that network. If we receive a SYN/ACK response, we know the port is **open**.

Introduction to SYN Scan

This enumeration process of sending SYN requests to many ports on a network is called a SYN Scan.

A SYN Scan is typically run by a software program that automates the sending of the SYN requests.

If a server responds with a SYN/ACK response, the client will not complete the three-way handshake with an ACK response.

The purpose of the SYN Scan is to determine the states of the ports on a network.

Port States

There are three main port states: **Open**, **closed**, and **filtered**.

01

Open means the port is accepting connections.

02

Closed means it is not accepting connections.

03

Filtered means it may be open, but a firewall or another network device is likely blocking it.

We can use Wireshark to view request and response conversations in order to determine if ports are open, closed or filtered.

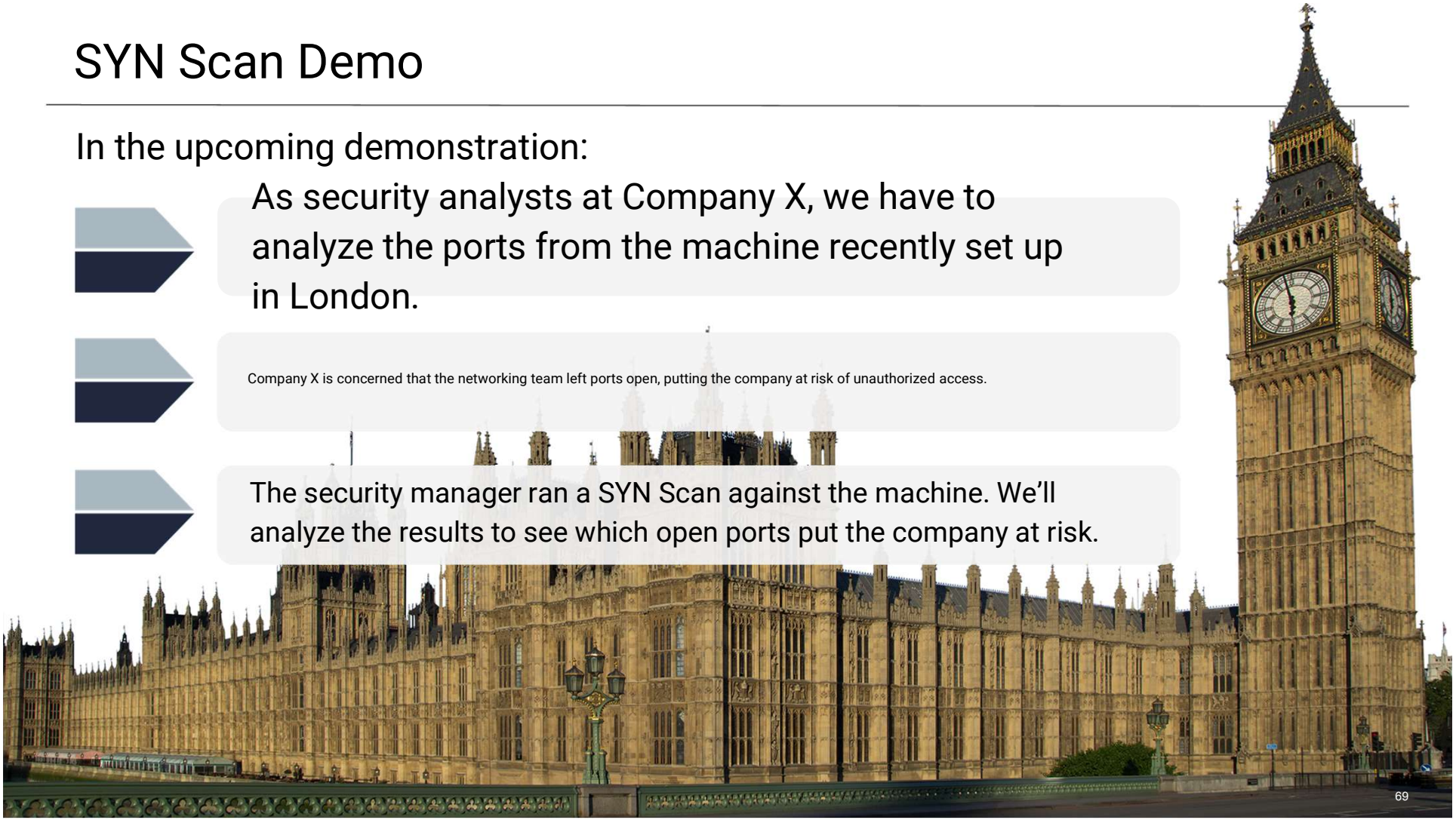
SYN Scan Demo

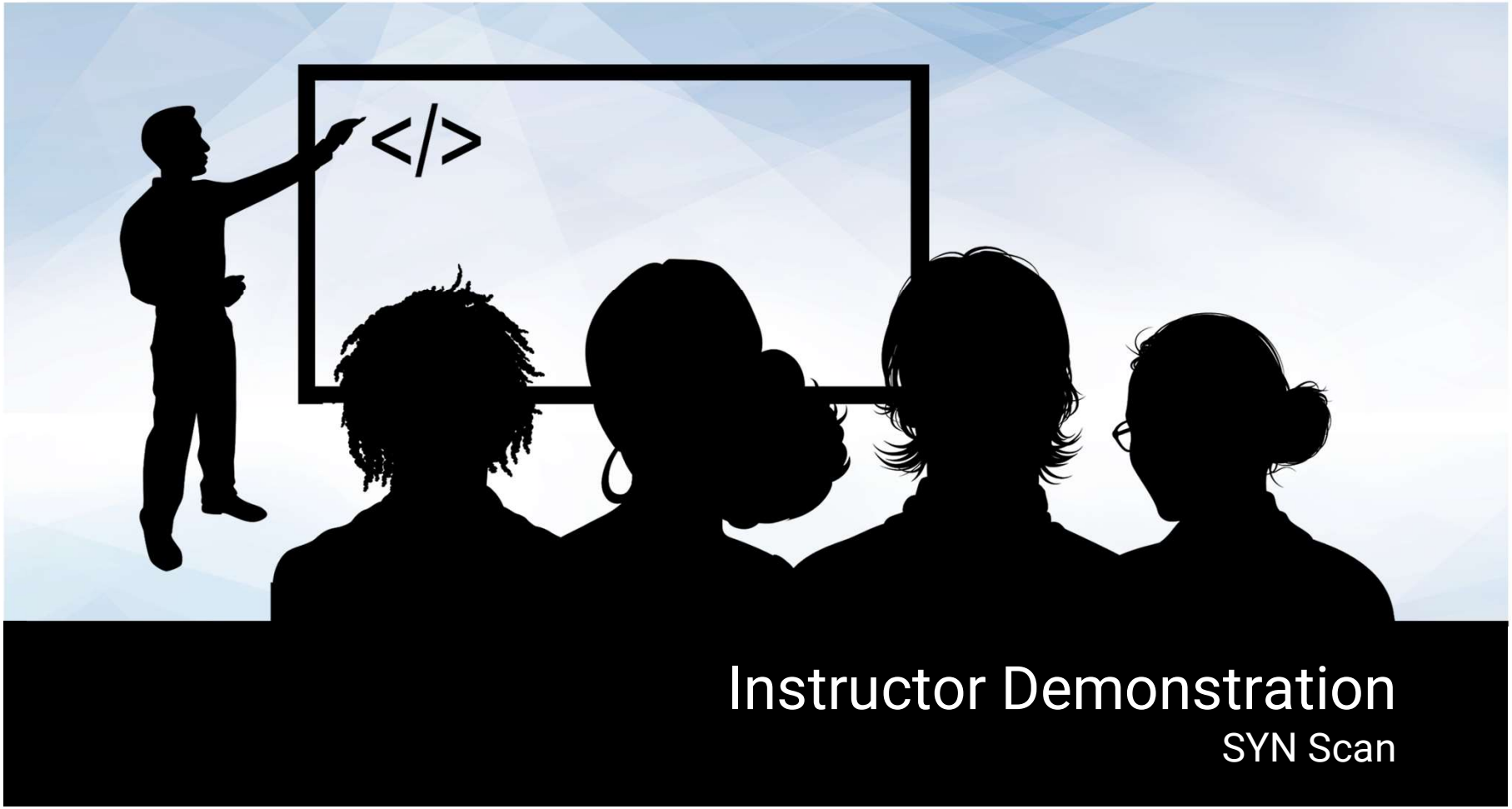
In the upcoming demonstration:

As security analysts at Company X, we have to analyze the ports from the machine recently set up in London.

Company X is concerned that the networking team left ports open, putting the company at risk of unauthorized access.

The security manager ran a SYN Scan against the machine. We'll analyze the results to see which open ports put the company at risk.



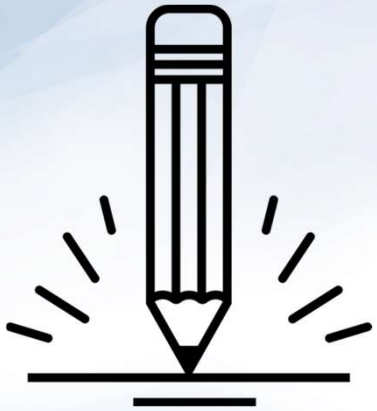

Instructor Demonstration
SYN Scan

SYN Scan Demo Summary

All of the SYN requests going from port to port was expected. We knew a SYN Scan was run by the security manager.

If a SYN SCAN wasn't planned, it is unusual network activity that should be looked into.

If a security professional saw this activity, they'd consider using a firewall to block the source IP from scanning the network. A hacker can use the same SYN Scan process for malicious reasons.



Activity: Analyzing a SYN Scan

CompuCom has hired you to do a security assessment of their network.

You will analyze a packet capture of a SYN Scan CompuCom ran against one of its hosts. You must determine what ports are open, closed, and filtered.

Suggested Time:
12 Minutes

Time’s Up! Let’s Review.

Class Objectives

By the end of today's class, you will be able to:

- Define enumeration as a set of methods used by security professionals and hackers to determine network vulnerabilities.
- Use Wireshark to visualize and analyze ARP activity, including ARP spoofing.
- Use `ping` and `fping` to determine if hosts are operating and accepting connections.
- Use `traceroute` to troubleshoot networking communication issues between two devices.
- Define and distinguish between TCP and UDP.
- Analyze TCP traffic in Wireshark.
- Analyze SYN Scans to determine the availability of ports on a network.